COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 42, No. 1 1993

ed. RIKKYO UNIV/MATH
IKEBUKURO TOKYO
171 JAPAN

Plane Quartics and Mordell-Weil Lattices of Type E_7

Dedicated to Professor S. Koizumi for his 70th birthday

by

Tetsuji SHIODA

(Received February 5, 1993)

In this paper, we consider the classical topic of the 28 bitangents of a plane quartic curve from the viewpoint of Mordell-Weil lattices of type E_7. We shall prove the results announced in our ICM report [S5], §8, 3); we refer to it also for the general idea of Mordell-Weil lattices.

Table of Contents

1. Normal forms

Let Γ be a smooth quartic curve in a projective plane $\boldsymbol{P}^2$ (in short: a smooth plane quartic). For any point $\xi \in \Gamma$, let T_ξ be the tangent line to Γ at ξ. In general, we have

$$\Gamma \cdot T_\xi = 2\xi + \xi' + \xi'' \quad (\text{for some } \xi', \xi'' \in \Gamma).$$

($A \cdot B$ means the intersection product of two curves A, B in $\boldsymbol{P}^2$.) A point $\xi \in \Gamma$ is called a *flex* if

$$\Gamma \cdot T_\xi = 3\xi + \xi' \quad (\text{for some } \xi' \in \Gamma).$$

A line L in $\boldsymbol{P}^2$ is called a *bitangent* (or a *double tangent*) of Γ if

$$\Gamma \cdot L = 2\xi + 2\xi' \quad (\text{for some } \xi, \xi' \in \Gamma).$$

It is wellknown that there are 28 bitangents and 24 flexes for any smooth plane quartic (e.g. [Mu], pp. 9–10 for the classical case). In more intrinsic terms, every non-hyperelliptic curve of genus 3 is embedded as a smooth plane quartic via the canonical map (i.e. the rational map associated with the canonical system) so that

the intersection of the quartic with lines are precisely effective canonical divisors. Thus a bitangent, for example, corresponds to an effective divisor of degree two $D=\xi+\xi'$ such that $2D$ is a canonical divisor.

Now let us consider a *normal form* of the pair (Γ, ξ), a plane quartic Γ with a chosen flex ξ. There are 2 cases to be distinguished:

$$\begin{cases} \text{(I)} & \Gamma\cdot T_\xi=3\xi+\xi' \quad (\xi\neq\xi') \\ \text{(II)} & \Gamma\cdot T_\xi=4\xi\,. \end{cases}$$

A flex ξ is said to be *ordinary* or *special* according to (I) or (II). To have some idea, here are explicit examples in both cases:

$$\text{(i)} \quad \Gamma: x_0^3x_1+x_1^3x_2+x_2^3x_0=0\,, \quad \xi=(0,0,1) \quad T_\xi: x_0=0\,.$$

$$\text{(ii)} \quad \Gamma: x_1^4+x_0^3x_2+x_2^3x_0=0\,, \quad \xi=(0,0,1)\,, \quad T_\xi: x_0=0\,.$$

A flex ξ is special if and only if the flex tangent T_ξ is at the same time a bitangent.

We say that (Γ, ξ) is defined over a field k if Γ is a curve defined over k and ξ is a k-rational point. In the following propositions, a plane quartic Γ is allowed to have singular points, although the chosen flex ξ is always assumed to be a smooth point of Γ. The condition for smoothness of Γ will be discussed later (see Theorem 5).

PROPOSITION 1. *Let k be arbirary field of characteristic $\neq 3$. Given a plane quartic with an ordinary flex (Γ, ξ) defined over k, there is a coordinate system (x_0, x_1, x_2) of $\boldsymbol{P}^2$ such that Γ, ξ are given by*

$$x_0x_2^3+x_2(p_0x_0^3+p_1x_0^2x_1+x_1^3)+q_0x_0^4+q_1x_0^3x_1+q_2x_0^2x_1^2+q_3x_0x_1^3+q_4x_1^4=0 \tag{1.1}$$
$$\xi=(0,0,1)\,, \qquad T_\xi: x_0=0\,.$$

Moreover the parameter

$$\lambda=(p_0, p_1, q_0, q_1, q_2, q_3, q_4)\in k^7$$

is uniquely determined up to the equivalence:

$$\lambda=(p_i, q_j)\sim\lambda'=(p_i', q_j') \Longleftrightarrow \tag{1.2}$$
$$p_i'=u^{6-2i}p_i \ (i=0,1)\,, \quad q_j'=u^{9-2j}q_j \ (j=0,1,\cdots,4) \text{ for some } u\neq 0.$$

PROPOSITION 2. *Let k be arbitrary field of characteristic $\neq 2$. Given a plane quartic with a special flex (Γ, ξ) defined over k, there is a coordinate system (x_0, x_1, x_2) of $\boldsymbol{P}^2$ such that Γ, ξ are given by*

$$x_0x_2^3+x_2(p_0x_0^3+p_1x_0^2x_1+p_2x_0x_1^2)+q_0x_0^4+q_1x_0^3x_1+q_2x_0^2x_1^2+x_1^4=0 \tag{1.3}$$
$$\xi=(0,0,1)\,, \qquad T_\xi: x_0=0\,.$$

Moreover the parameter

$$\lambda=(p_0, p_1, p_2, q_0, q_1, q_2)\in k^6$$

is uniquely determined up to the equivalence:

$$\lambda=(p_i, q_j)\sim\lambda'=(p'_i, q'_j)\Longleftrightarrow \tag{1.4}$$
$$p'_i=u^{8-3i}p_i\ (i=0, 1, 2)\,,\quad q'_j=u^{12-3j}q_j\ (j=0, 1, 2)\ \textit{for some}\ u\neq 0\,.$$

DEFINITION. We call a curve with the equation $F(x_0, x_1, x_2)=0$ of the form (1.1) or (1.3) the *normal form* of a plane quartic with a flex (ordinary or special), which will be denoted by Γ_λ in the sequel.

An immediate consequence of Proposition 1 is the following rationality of the moduli space:

THEOREM 3. *The moduli space of plane quartics with a flex is a rational variety of dimension* 6 *over any base field of characteristic* $\neq 3$.

Indeed, a flex of a plane quartic is generically an ordinary flex. Then, in the normal form (1.1), the coefficient q_4 is generically not equal to 0. In this case, we can uniquely normalize λ by letting $q_4=1$. Thus we obtain a generic one-one correspondence

$$\text{isomorphism class of } (\Gamma, \xi)\leftrightarrow(p_0, p_1, q_0, q_1, q_2, q_3)\in k^6$$

which proves the assertion.

To prove Propositions 1 and 2, we first choose a coordinate system x_i so that the given flex ξ has the coordinates (0, 0, 1) and the tangent line T_ξ is defined by $x_0=0$. When we write the defining equation of Γ as

$$F(x_0, x_1, x_2)=A_0x_2^4+A_1x_2^3+A_2x_2^2+A_3x_2+A_4=0\,,$$

where A_d is a binary form of degree d in x_0, x_1, the polynomial $F(0, x_1, 1)$ must be divisible by x_1^3. This implies that $A_0=0$, $A_1=cx_0$, $A_2=x_0B_1$ for some constant $c\neq 0$ and some linear form B_1. Then we can take $c=1$ and $A_2=0$ by dividing F by c and replacing x_2 by $x_2-B_1/3c$ (using char $\neq 3$). Thus we have

$$F=x_0x_2^3+x_2\sum_{i=0}^{3}p_ix_0^{3-i}x_1^i+\sum_{j=0}^{4}q_jx_0^{4-j}x_1^j$$

with some coefficients $p_i, q_j\in k$. Now it follow from

$$F(0, x_1, x_2)=(p_3x_2+q_4x_1)x_1^3$$

that $(p_3, q_4)\neq(0, 0)$ and that ξ is an ordinary flex if and only if $p_3\neq 0$. At this stage, we still have freedom in changing the coordinates (a) $x_i\to c_ix_i$ $(c_i\neq 0)$ or (b) $x_1\to x_1+cx_0$.

(I) Now suppose that ξ is an ordinary flex. Then we have $p_3\neq 0$. By a coordinate change of type (a), p_3 is replaced by $p'_3=p_3c_1^3/c_0c_2^2$. Hence, by a suitable choice of c_i, we can take $p_3=1$. Then we can kill the coefficient p_2 by a coordinate change of type (b) (again using char $\neq 3$). Thus we have arrived at the normal form (1.1) stated in Proposition 1. The remaining freedom is the choice of c_i satisfying $c_1^3=c_0c_2^2$, i.e.

$(c_0 : c_1 : c_2) = (1 : u^{-2} : u^{-3})$ for some $u \neq 0$. Thus the parameter $\lambda = (p_i, q_j)$ is uniquely determined up to the equivalence (1.2) in Proposition 1.

(II) Next suppose that ξ is a special flex. Then we have $p_3 = 0$, $q_4 \neq 0$. As before, by a coordinate change of type (a), q_4 is replaced by $q'_4 = q_4 c_1^4 / c_0 c_2^3$. Hence, by a suitable choice of c_i, we can take $q_4 = 1$. Then we can kill the coefficient q_3 by a coordinate change of type (b) (using char $\neq 2$). Thus we obtain the normal form (1.3) stated in Proposition 2. The remaining freedom is the choice of c_i satisfying $c_1^4 = c_0 c_2^3$, i.e. $(c_0 : c_1 : c_2) = (1 : u^{-3} : u^{-4})$ for some $u \neq 0$. Thus the parameter $\lambda = (p_i, q_j)$ is uniquely determined up to the equivalence (1.4) in Proposition 2.

This completes the proof of Propositions 1 and 2.

2. Mordell-Weil lattices of type E_7

From now on, we assume that k is an algebraically closed field of characteristic $\neq 2, 3$. Let (Γ, ξ) be a plane quartic with an ordinary flex. By Proposition 1, we can suppose without loss of generality that Γ is equal to Γ_λ having the normal form

$$\begin{aligned} F(x_0, x_1, x_2) = {} & x_0 x_2^3 + x_2(p_0 x_0^3 + p_1 x_0^2 x_1 + x_1^3) + q_0 x_0^4 + q_1 x_0^3 x_1 \\ & + q_2 x_0^2 x_1^2 + q_3 x_0 x_1^3 + q_4 x_1^4 = 0 \end{aligned} \tag{2.1}$$

with the parameter

$$\lambda = (p_0, p_1, q_0, q_1, q_2, q_3, q_4) \in k^7 .$$

In terms of the inhomogeneous coordinates

$$t = \frac{x_1}{x_0}, \qquad x = \frac{x_2}{x_0},$$

the curve Γ_λ has an affine equation

$$F_{aff} = x^3 + x(p_0 + p_1 t + t^3) + (q_0 + q_1 t + q_2 t^2 + q_3 t^3 + q_4 t^4) = 0 . \tag{2.2}$$

Let us consider a closely related equation:

$$y^2 = x^3 + x(p_0 + p_1 t + t^3) + (q_0 + q_1 t + q_2 t^2 + q_3 t^3 + q_4 t^4) , \tag{2.3}$$

which defines the following objects:

(i) an elliptic curve $E = E_\lambda$ over $k(t)$
(ii) an elliptic surface $f : S_\lambda \to \boldsymbol{P}^1$
(iii) an affine surface S'_λ in (x, y, t)-space.
(iv) a double cover V_λ of $\boldsymbol{P}^2$ ramified along the quartic Γ_λ.

We have studied (i), (ii) in detail in [S3], §9. The elliptic surface has a reducible singular fibre of type III at $t = \infty$ (a union of two smooth rational curves tangent at a single intersection point). Assume the following condition on λ:

(♯) there are no other reducible fibres than $f^{-1}(\infty)$.

Then, by [S1], II, Th. 2.1 or [S2], Th. 10.4, the Mordell-Weil group $E(k(t))$ is

torsionfree of rank 7 and it is isomorphic as a lattice to the dual lattice of the root lattice E_7:

$$E(k(t)) \simeq E_7^* \tag{2.4}$$

(see §5 for this lattice). Corresponding to the 56 minimal vectors of norm 3/2 in E_7^*, there are 56 $k(t)$-rational points $P=(x, y)$ of the form:

$$x=at+\mathrm{b}\,, \qquad y=ct^2+dt+e \tag{2.5}$$

([S3], Lemma 9.1). Since $-P=(x, -y)$, we can arrange them as $\pm P_n$ $(n=1, \cdots, 28)$. Moreover we can choose $\{P_1, \cdots, P_7\}$ to form a basis of $E(k(t)) \simeq E_7^*$. Observe that, if we write

$$P_n=(a_nt+b_n,\ c_nt^2+d_nt+e_n) \qquad (n=1, \cdots, 28)\,, \tag{2.6}$$

then the 28 values $x=a_nt+b_n$ are mutually distinct.

In terms of the homogeneous coordinates x_i, (2.5) is equivalent to the identity:

$$F(x_0, x_1, ax_1+bx_0)=(cx_1^2+dx_1x_0+ex_0^2)^2\,, \tag{2.7}$$

which clearly shows that the line $x_2=ax_1+bx_0$ is a bitangent of Γ. Conversely, any bitangent can be obtained this way. (Otherwise, its equation would be of the form $ax_1+bx_0=0$ for some a, b, not both 0. In case $a\neq 0$, F_{aff} would be a square when we let $t=-b/a$, which is impossible. On the other hand, if $a=0$, then the line $x_0=0$ would be a bitangent. But this is again impossible since $x_0=0$ is the tangent line at the ordinary flex ξ by Proposition 1.) Therefore we have proven the following:

PROPOSITION 4. *Under the condition* (♯), *the plane quartic* Γ_λ *has exactly* 28 *bitangents, which are given by the lines*

$$l_n : x_2=a_nx_1+b_nx_0 \qquad (n=1, \cdots, 28)\,, \tag{2.8}$$

and the two points of contact on each line l_n *are determined by*

$$c_nx_1^2+d_nx_1x_0+e_nx_0^2=0\,. \tag{2.9}$$

Now a natural question is the relationship of the condition (♯) and the smoothness of the plane quartic Γ_λ. The answer is contained in:

THEOREM 5. *The following* 9 *conditions on* λ *are mutually equivalent*:

(0) *The plane quartic* Γ_λ *is smooth.*

(0′) Γ_λ *has* 28 (*distinct*) *bitangents.*

(1) *The Mordell-Weil lattice* $E_\lambda(k(t))$ *is isomorphic to* E_7^*.

(1′) $E_\lambda(k(t))$ *contains* 56 *rational points of the form* (2.5).

(1″) $\mathrm{rk}\, E_\lambda(k(t))=7$.

(2) (=(♯)) *The elliptic surface* $f: S_\lambda \to \boldsymbol{P}^1$ *has no reducible fibres other than* $f^{-1}(\infty)$.

(3) *The affine surface* S'_λ *is smooth.*

(4) *The double cover* V_λ *is smooth* (*a del Pezzo surface of degree* 2).

(5) *The discriminant* $\delta_0(\lambda)\neq 0$. (*See* §5 *below for the definition of* δ_0, *which is an invariant of weight* 126.)

Proof. The equivalence of (0) and (0′) is classically wellknown by Plücker's formula. For the equivalence of the conditions (1), (1′), (1″), (2), (3), (5), we refer to [S3], §9 (cf. also [S2] and [S4]). Now the argument before Proposition 4 shows that (0′) and (1′) are equivalent. Finally it is wellknown (and easily seen) that a double cover of $\boldsymbol{P}^2$ ramified along a curve of even degree has a singularity exactly over a singular point of the curve. Hence (0) and (4) are equivalent. (For del Pezzo surfaces, see [Ma], Ch. 4.) Thus all conditions are shown to be equivalent.

N.B. We note that (2) and (4) are more directly related, i.e. the elliptic surface $S=S_\lambda$ and the surface V_λ are related as follows. The zero section (O) of S is an exceptional curve of the first kind, and the two irreducible components of $f^{-1}(\infty)$ are smooth rational curves with self-intersection -2. When we blow down (O), we have a birational morphism $\beta_1: S\to S_1$ (with S_1 smooth), under which the irreducible component of $f^{-1}(\infty)$ meeting (O) is mapped to an exceptional curve of the first kind on S_1. Hence, by blowing it down, we obtain $\beta_2: S_1\to S_2$ with S_2 smooth. Under the condition (2), S_2 is a (smooth) del Pezzo surface of degree 2, which is nothing but the surface V_λ. There are exactly 56 exceptional curves of the first kind on a del Pezzo surface of degree 2, which are mapped in pairs to the 28 bitangents of the quartic Γ_λ.

3. The Galois group of 28 bitangents

Let $\mathscr{B}$ denote the smallest field of rationality of all the bitangents of Γ_λ. Then it follows from Proposition 4 that $\mathscr{B}$ is generated over the coefficient field $\kappa(\lambda)$ by a_n, b_n $(n=1, \cdots, 28)$, where κ denotes the prime field in k. That is:

$$\mathscr{B}=\kappa(\lambda)(a_n, b_n \,|\, n=1, \cdots, 28) \tag{3.1}$$

The viewpoint of Mordell-Weil lattices has revealed, however, that the most essential parameter of a bitangent l is the "hidden coefficient" c rather than a or b (see [S3], §9, for what follows). Indeed, as will be seen below, this observation throws some new light on this old, well-studied topic of bitangents of a plane quartic.

To explain this, we recall some results from [S3], §9. We keep the notation in the previous sections: $P_n, a_n, b_n, c_n, \cdots$. In addition, we assume that $\{P_1, \cdots, P_7\}$ forms a basis of $E(k(t))\simeq E_7^*$. First we work in characteristic 0, i.e. let $\kappa=\boldsymbol{Q}$.

Let $\mathscr{K}$ denote the splitting filed of $E(k(t))$, i.e. the smallest extension of $k_0=\boldsymbol{Q}(\lambda)$ such that $E(k(t))=E(\mathscr{K}(t))$; this is a finite Galois extension. Since P_n $(n\leq 28)$ (indeed P_n $(n\leq 7)$) generate $E(k(t))$, we have

$$\mathscr{K}=k_0(a_n, b_n, c_n, c_n, e_n \,|\, n=1, \cdots, 28)\,. \tag{3.2}$$

In particular, the field of the bitangents $\mathscr{B}$ is contained in $\mathscr{K}$:

$$\mathscr{B}\subset\mathscr{K}\,. \tag{3.3}$$

LEMMA 6. *The extension $\mathscr{K}/\mathscr{B}$ is at most quadratic*: $[\mathscr{K}:\mathscr{B}]\leq 2$.

Proof. Suppose that an automorphism σ of $\mathscr{K}$ is trivial on $\mathscr{B}$. Then it fixes the x-coordinate of each P_n and hence we have

$$P_n^\sigma=\eta_n P_n\,,\qquad \eta_n=\pm 1\,.$$

We claim that the sign η_n is independent of $n=1,\cdots,28$. In fact, by a general property of the height pairing ([S2], Prop. 8.13), we have

$$\langle P_n^\sigma, P_{n'}^\sigma\rangle=\langle P_n, P_{n'}\rangle\,.$$

On the other hand, the explicit formula for the pairing ([S2], Th. 8.6) implies

$$\langle P_n, P_{n'}\rangle=1-(P_n, P_{n'})-\frac{1}{2}\neq 0$$

for any n, n'. Hence we have $\eta_n\cdot\eta_n'=1$, proving the claim. It follows that the Galois group of $\mathscr{K}/\mathscr{B}$ is contained in $\{\pm 1\}$. q.e.d.

Suppose that λ is generic (i.e. p_i, q_j are algebraically independent) over $\boldsymbol{Q}$. By Theorem 9.4, [S3], we have

$$\mathscr{K}=\boldsymbol{Q}(c_1,\cdots,c_{28})=\boldsymbol{Q}(c_1,\cdots,c_7) \tag{3.4}$$

where $c_1,\cdots,c_7$ are algebraically independent and all other c_n are $\boldsymbol{Z}$-linear combination of them. (The latter follows from the fact that the map $P_n\to c_n$ is induced by a group homomorphism $E(k(t))\to k$ called the specialization map.) There is a *universal polynomial of type E_7*:

$$\Phi(X,\lambda)=X^{56}-36q_4X^{54}+\cdots\in\boldsymbol{Z}[\lambda][X] \tag{3.5}$$

whose roots are precisely $\pm c_n$ ($n=1,\cdots,28$), i.e.

$$\Phi(X,\lambda)=\prod_{n=1}^{28}(X^2-c_n^2)\,.$$

Further we know that $\mathscr{K}$ is a Galois extension of $k_0=\boldsymbol{Q}(\lambda)=\boldsymbol{Q}(p_0,\cdots,q_4)$ with Galois group $W(E_7)$, the Weyl group of type E_7. The relation of roots and coefficients for the universal polynomial identifies p_i, q_j with the *explicit fundamental invariants* of $W(E_7)$ of respective weight

$$wt(p_i)=12-4i\ (i=0,1)\,,\quad wt(q_j)=18-4j\ (j=0,\cdots,4)\quad (cf.\ (1.2)) \tag{3.6}$$

See (6.1) below for the explicit formulas which are reproduced from [S3], p. 684. In particular, we have

$$\boldsymbol{Q}[c_1,\cdots,c_7]^{W(E_7)}=\boldsymbol{Q}[p_0,\cdots,q_4]\,. \tag{3.7}$$

Moreover the same results as above hold if $\boldsymbol{Q}$ is replaced by any base field of characteristic $\neq 2, 3, 5, 7, 11, 29, 1229$ (cf. [S3], p. 690 and (3.11) below).

Now we conclude that for λ generic over κ, $\mathscr{B}$ is the Galois extension of $k_0=\kappa(\lambda)$

corresponding to the subgroup $\{\pm 1\}$ of $W(E_7)$. Hence the Galois group of $\mathscr{B}/k_0$ is the quotient group $W(E_7)/\{\pm 1\}$, which is known to be isomorphic to $Sp(6, \boldsymbol{Z}/2\boldsymbol{Z})$, a simple group of order $2^9 3^4 5 \cdot 7 = 1451520$ (denoted as $S_6(2)$ in [A]). In summary:

THEOREM 7. *The Galois group of* 28 *bitangents of the plane quartic* Γ_λ *is the simple group* $Sp(6, \boldsymbol{Z}/2\boldsymbol{Z})$, *at least if* λ *is generic over the prime field in characteristic* $\neq 2$, 3, 5, 7, 11, 29, 1229.

This result is a refinement of the wellknown fact on the Galois group of 28 bitangents of a generic plane quartic whose study goes back to the middle 19th century, right after the birth of Galois theory (cf. [W], [vW]). By taking more general defining equations, the restriction on the characteristic can be removed, but we don't go into it.

Instead, let us make the extension $\mathscr{B}/k_0$ more explicit and write down the *algebraic equation of* 28 *bitangents*. Recall that all the coefficients $a_n, b_n, \cdots$ of P_n belong to the splitting field $\mathscr{K}$. Explicitly, this comes about as follows. Substituting (2.5) into (2.3) and comparing the coefficients of $t^4, t^3, \cdots$, we get 5 relations of a, b, c, d, e over $k_0 = \kappa(\lambda) = \kappa(p_i, q_j)$:

$$\text{(3.8)} \qquad \begin{cases} a &= c^2 - q_4 \\ b &= 2cd - a^3 - q_3 \\ 2ce &= -d^2 + 3a^2 b + p_1 a + q_2 \\ 2de &= 3ab^2 + p_0 a + p_1 b + q_1 \\ e^2 &= b^3 + p_0 b + q_0 \end{cases}.$$

The first 3 relations express a, b, e as elements of $k_0(c, d)$, and then the last 2 relations give monic relations of d over $k_0(c)$:

$$\text{(3.9)} \qquad d^3 + \cdots = 0\,, \qquad d^4 + \cdots = 0\,.$$

Eliminating d, we obtain a monic relation of degree 56 in c over k_0, which is nothing but the universal polynomial $\Phi(c, \lambda)$. For each $c = c_n$ $(n = 1, \cdots, 28)$, we have

$$\text{(3.10)} \qquad a_n = c_n^2 - q_4\,.$$

On the other hand, $d = d_n$ is a rational function of c with coefficients in k_0 which is also expressed as a polynomial in $\kappa[c_1, \cdots, c_7]$ ([S3], Th. 9.5). Similarly $b = b_n$ can be expressed as a rational function of $a = a_n$ with coefficients in k_0 which is also an even polynomial in $\kappa[c_1, \cdots, c_7]$. (It is not practical to print these expressions here.) With these notation, we have:

THEOREM 8. *The field of bitangents is generated by* $\{a_1, \cdots, a_7\}$ *over* k_0:

$$\text{(3.11)} \qquad \mathscr{B} = k_0(a_1, \cdots, a_{28}) = k_0(a_1, \cdots, a_7)\,,$$

and it is the splitting field of the algebraic equation with coefficients in $\boldsymbol{Z}[\lambda]$:

$$\begin{aligned}\Psi(a,\lambda)=&a^{28}-8q_4a^{27}+72q_3a^{25}+60p_1a^{24}-(504q_2-432p_1q_4)a^{23}\\&-(540p_0+\cdots)a^{22}+(3828q_1+\cdots)a^{21}+\cdots\\&-(29496q_0+\cdots)a^{19}+\cdots=0\end{aligned}\tag{3.12}$$

Proof. Suppose an automorphism σ of $\mathscr{K}/k_0$ fixes $a_1, \cdots, a_7$. Then it fixes the x-coordinate a_it+b_i of P_i for $i=1, \cdots, 7$. Hence each P_i is mapped to $\pm P_i$ under σ. By the same argument as in Lemma 6, we see that the sign is independent of i. Since $P_1, \cdots, P_7$ generate $E(k(t))$, this implies $\sigma=\pm 1$ in $W(E_7)$. By Galois theory, $k_0(a_1, \cdots, a_7)$ coincides with $\mathscr{B}$. This proves the first assertion. As for the second, note that the universal polynomial $\Phi(c, \lambda)$ is a polynomial in c^2. Hence the substitution $c^2=a+q_4$ turns it into a polynomial in a of degree 28 with coefficients in k_0 (or more precisely, in $\boldsymbol{Z}[\lambda]$), which is nothing but $\Psi(a, \lambda)$. q.e.d.

As a standard application, the above theorem (in char 0) combined with Hilbert's irreducibility theorem ([L], [Se]) implies the existence of plane quartics over $\boldsymbol{Q}$ (or its finite extensions) for which the Galois group of 28 bitangents is as big as possible, i.e. equal to $Sp(6, \boldsymbol{Z}/2\boldsymbol{Z})$. More interesting is the observation that our method is effective, that is, we can write down explicit numerical examples for such.

Example ("big Galois"). For the plane quartic over $\boldsymbol{Q}$ with the coefficients $p_0=p_1=q_0=q_1=q_2=q_4=1$, $q_3=0$:

$$x_0x_2^3+x_2(x_0^3+x_0^2x_1+x_1^3)+x_0^4+x_0^3x_1+x_0^2x_1^2+x_1^4=0\,,$$

the Galois group of 28 bitangents over $\boldsymbol{Q}$ is equal to $Sp(6, \boldsymbol{Z}/2\boldsymbol{Z})$. The field of bitangents $\mathscr{B}$ is the splitting field of the algebraic equation of degree 28:

$$\begin{aligned}\Psi(a)=&a^{28}-8a^{27}+60a^{24}-72a^{23}-1404a^{22}-876a^{21}+10350a^{20}\\&-4560a^{19}-169764a^{18}-490716a^{17}-684758a^{16}-513500a^{15}\\&-202038a^{14}+25940a^{13}+2521709a^{12}+11389944a^{11}+22683596a^{10}\\&+24787712a^9+17436690a^8+12663696a^7+13086010a^6+11193468a^5\\&+5987941a^4+2134648a^3+700246a^2+208572a+26633=0\,.\end{aligned}$$

See [S5], Ex. 7.6, where the corresponding result for $\mathscr{K}$ is sketched.

In the other extreme, the Galois group in question can be trivial ("small Galois"), i.e. all the bitangents are rational over the field of definition of the quartic. A systematic construction of such a quartic will be discussed in §6. Before that, let us treat the case of the Klein quartic over $\boldsymbol{Q}$ as an example with "intermediary" Galois group. Of course, the result should be wellknown.

4. Bitangents of the Klein quartic

Consider the Klein quartic over $\boldsymbol{Q}$:

(4.1) $$F=x_0^3x_1+x_1^3x_2+x_2^3x_0=0\,.$$

In the previous notation, we have $q_1=1$, $p_0=p_1=0$, $q_j=0$ $(j\neq 1)$.

First we evaluate the polynomials $\Phi(c,\lambda)$, $\Psi(a,\lambda)$. To simplify the notation, we go back to the inhomogeneous coordinates x, y, t. Substituting $x=at+b$ into $F=x^3+xt^3+t$, we have (cf. (2.3) and (2.5))

$$(at+b)^3+(at+b)t^3+t=(ct^2+dt+e)^2\,.$$

In this case, (3.8) reduces to

$$a=c^2,\ b+a^3=2cd,\ \cdots,\ b^3=e^2\,.$$

Eliminating a, b, e, d from the above (in this order), we obtain a monic equation of degree 56 in c:

(4.2) $$\Phi(c)=c^{56}+3828c^{42}+87462c^{28}+83636c^{14}+1\,,$$

which is nothing but the universal polynomial evaluated for the present p_i, q_j. Since $a=c^2$, the "algebraic equation for bitangents" of degree 28 is given by $\Psi(a)=a^{28}+\cdots+1$.

Letting $U=c^{14}=a^7$, we obtain a degree 4 polynomial in U, which factors as

(4.3) $$(U+1)(U^3+3827U^2+83635U+1)\,.$$

The first factor gives $a^7=-1$, which correspond to the 7 bitangents with $-a$ 7th root of unity. The bitangent with $a=-1$ is given by

$$l_0: x_2=-x_0-x_1\,,\quad \text{i.e.,}\quad x_0+x_1+x_2=0\,.$$

Indeed, it is easy to check that

$$F(x_0, x_1, -x_0-x_1)=-(x_0^2+x_0x_1+x_1^2)^2\,.$$

On the other hand, the projective transformation

(4.4) $$g_\zeta: (x_0, x_1, x_2)\to(\zeta^3x_0, \zeta x_1, x_2)$$

induces an automorphism of order 7 of the Klein curve if ζ is a primitive 7th root of unity. The bitangents with $a^7=-1$ are tranforms of l_0 under these automorphisms.

Next we consider the cubic factor in (4.3). Its splitting field turns out to be the real cubic field $\boldsymbol{Q}(\zeta_7)^+=\boldsymbol{Q}(\varepsilon)\subset\boldsymbol{Q}(\zeta_7)$, where we let $\zeta_7=e^{2\pi i/7}$ and $\varepsilon=\zeta_7+\zeta_7^{-1}$. Obviously the 3 roots, say U_i $(i=1, 2, 3)$, are units. Introduce the standard units in $\boldsymbol{Q}(\zeta_7)^+$:

$$\begin{cases}\varepsilon_1=\varepsilon & =2\cos(2\pi/7)\\ \varepsilon_2=\varepsilon^\sigma & =2\cos(4\pi/7)\\ \varepsilon_3=\varepsilon^{\sigma^2}=2\cos(8\pi/7)\end{cases}$$

where σ is the Galois automorphism of $\boldsymbol{Q}(\zeta_7)$ defined by $\zeta_7\to\zeta_7^2$. Then we can identify the 3 roots in question to be

(4.5) $$U_1=-\varepsilon_1^{14},\quad U_2=-\varepsilon_2^{14},\quad U_3=-\varepsilon_3^{14}.$$

It is not so trivial to find out these relation, although this kind of phenomenon has appeared before (cf. [S1], II, §4 and [S4], Prop. 7.2). But the verification is straightforward, so we omit it. Solving $a^7=U_i$, we obtain

$$a=-\zeta_7^j\varepsilon_i^2 \qquad (i=1, 2, 3; j=0, 1, \cdots, 6).$$

To determine the equation of a bitangent $x=at+b$, we need to know b. It is easy to see that $1/b$ has a similar expression as above, by noting that the bitangents are permuted among themselves by the cyclic automorphism $(x_0, x_1, x_2)\to(x_1, x_2, x_0)$. In this way, we find 3 real bitangents

$$\begin{cases} l_1: x_2=-\varepsilon_1^2x_1-\varepsilon_3^{-2}x_0 \\ l_2: x_2=-\varepsilon_2^2x_1-\varepsilon_1^{-2}x_0 \\ l_3: x_2=-\varepsilon_3^2x_1-\varepsilon_2^{-2}x_0 \end{cases}.$$

Again the verification is not too hard.

Finally, each of l_i $(i=0, 1, 2, 3)$ has 7 transforms under the automorphisms g_ζ^j, and thus we have obtained all the 28 bitangents of the Klein quartic. Note that the field of bitangents is $\boldsymbol{Q}(\zeta_7)$, while the splitting field of $\Phi(c)$ is equal to $\boldsymbol{Q}(\zeta_7, i)$.

Now the Klein quartic remains nonsingular in every characteristic $p\neq 7$. Since the results obtained above are of integral nature (i.e. all the coefficients are contained in $\boldsymbol{Z}[\zeta]$), we can take the reduction mod p of the resulting formulas. Thus we can summarize the above in the following way:

PROPOSITION 9. *Let κ be the prime field of characteristic $p\geq 0$, $p\neq 7$, and consider the Klein quartic $x_0^3x_1+x_1^3x_2+x_2^3x_0=0$ over κ. Fix a primitive 7th root of unity ζ over κ, and set $\varepsilon_1=\zeta+\zeta^{-1}$, $\varepsilon_2=\zeta^2+\zeta^{-2}$, $\varepsilon_3=\zeta^4+\zeta^{-4}$. Then the 28 bitangents are given by*

(4.6) $$\begin{cases} l_{0,j}: x_2=-\zeta^jx_1-\zeta^{3j}x_0 \\ l_{1,j}: x_2=-\zeta^j\varepsilon_1^2x_1-\zeta^{3j}\varepsilon_3^{-2}x_0 \\ l_{2,j}: x_2=-\zeta^j\varepsilon_2^2x_1-\zeta^{3j}\varepsilon_1^{-2}x_0 \\ l_{3,j}: x_2=-\zeta^j\varepsilon_3^2x_1-\zeta^{3j}\varepsilon_2^{-2}x_0 \end{cases}$$

where $j=0, 1, \cdots, 6$.

In general, the field of rationality of bitangents and that of flexes for a given plane quartic seem to be quite different (perhaps linearly disjoint from each other in a generic case). But, in the case of the Klein quartic, they coincide. In fact, we have:

PROPOSITION 10. *The 24 flexes of the Klein quartic are given as follows. There are 3 special flexes (0, 0,1), (0, 1, 0), (1, 0,0) with the flex tangents $x_0=0$, $x_1=0$, $x_2=0$ forming the coordinate triangle. The remaining 21 flexes are:*

(4.7) $$(1, \zeta^j\varepsilon_1, \zeta^{3j}\varepsilon_3^{-1}),\quad (1, \zeta^j\varepsilon_2, \zeta^{3j}\varepsilon_1^{-1}),\quad (1, \zeta^j\varepsilon_3, \zeta^{3j}\varepsilon_2^{-1})\quad (j=0, 1, \cdots, 6)$$

Outline of Proof. As is wellknown, the flexes of a plane curve are the points of intersection of the curve with its Hessian (at least in characteristic 0). For the Klein quartic, the Hessian is given by

$$H=x_0x_1^5+x_1x_2^5+x_2x_0^5-5x_0^2x_1^2x_2^2$$

up to a nonzero constant multiple (if char $\neq 2, 3$). For any flex (x_0, x_1, x_2) other than the special 3, we have $x_i\neq 0$, so we may assume $x_0=1$. Then eliminating x_2 from $F=H=0$, we get an equation for x_1 of degree 21 which is written in terms of $u=x_1^7$ as

$$u^3+289u^2-57u-1=0\,.$$

A little work shows that the 3 roots of this equation are $u=1/\varepsilon_i^7$ $(i=1, 2, 3)$. The rest of the proof is similar to the previous one for bitangents, so we omit it.

N.B. It is wellknown that the automorphism group of the Klein quartic (in char 0) is a simple group of order 168, which is the largest order for curves of genus 3 in char 0. In the above, we used obvious automorphisms of order 7 or 3. If we use other automorphisms (all defined over $\boldsymbol{Q}(\zeta)$), then Proposition 6 or 7 can be proven without solving algebraic equations. Conversely, these results could be used to determine the automorphism group. For the connection with the modular curve of level 7, see [K].

5. Preliminaries on the lattice E_7^*

First let us recall some facts on the minimal vectors of the root lattice E_7 and its dual lattice E_7^*. To be concrete, we take the following realization of the root lattice E_7:

$$E_7=\left\{(x_1, \cdots, x_8)\,\middle|\,\sum_i x_i=0,\ 2x_i\in\boldsymbol{Z},\ x_i-x_j\in\boldsymbol{Z}\right\}\subset\boldsymbol{R}^8\,, \tag{5.1}$$

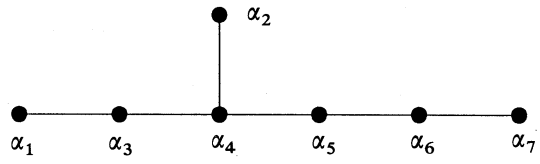
with the pairing induced from the standard metric $\sum_i x_i^2$ on $\boldsymbol{R}^8$. The minimal norm is 2, and the minimal vectors (of norm 2) are called "roots" for historical reason. There are 126 roots of which 56 are obtained from $(1, -1, 0, \cdots, 0)$ by permutation and 70 from $(1/2, 1/2, 1/2, 1/2, -1/2, -1/2, -1/2, -1/2)$. The Weyl group $W(E_7)$ is the automorphism group of the lattice E_7, and it acts transitively on the set of 126 roots. Following [CS], Ch. 4, we take a basis (or a set of simple roots) of E_7 as follows:

$$\alpha_1=(0, 0, 0, 0, 0, -1, 1, 0)\,,\qquad \alpha_2=\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{-1}{2}, \frac{-1}{2}, \frac{-1}{2}, \frac{-1}{2}\right),$$

$$\alpha_3=(0, 0, 0, 0, -1, 1, 0, 0)\,,\qquad \alpha_4=(0, 0, 0, -1, 1, 0, 0, 0),\qquad \cdots,$$

$$\alpha_7=(-1, 1, 0, 0, 0, 0, 0, 0)\,.$$

The information about $\langle\alpha_i, \alpha_j\rangle$ is expressed in a Dynkin diagram:



Then a half of roots ("positive roots") are nonnegative integral linear combination of $\alpha_1, \cdots, \alpha_7$. We call them α_m $(1 \leq m \leq 63)$ in some fixed order; e.g.

$$\text{(5.2)} \qquad \begin{cases} \alpha_8 = \alpha_1 + \alpha_3 , \\ \alpha_9 = \alpha_2 + \alpha_4 , \\ \cdots \\ \alpha_{63} = 2\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 3\alpha_5 + 2\alpha_6 + \alpha_7 . \end{cases}$$

(N.B. Since these linear expressions are independent of the choice of bases having the same diagram, we can use the information in the table (planche) VI of [B].)

Next we consider the dual lattice E_7^*. By definition, it is given by

$$\text{(5.3)} \qquad E_7^* = \{x \in E_7 \otimes \boldsymbol{Q} \mid \langle x, y \rangle \in \boldsymbol{Z}, \forall y \in E_7\}$$

which contains E_7 as a sublattice of index 2. We have $\det E_7^* = 1/\det E_7 = 1/2$. The minimal norm is 3/2, and the number of minimal vectors is 56. They are equal to $\pm(1/4, \cdots, 1/4, -3/4, -3/4)$ up to permutation; any one of them generate E_7^* modulo E_7. The action of $W(E_7)$ on 56 minimal vectors is again transitive. We set

$$\text{(5.4)} \qquad \begin{cases} u_1 = \frac{1}{4}(1, 1, 1, 1, 1, 1, -3, -3) \\ u_2 = \frac{1}{4}(1, 1, 1, 1, 1, -3, 1, -3) \\ u_3 = \frac{1}{4}(1, 1, 1, 1, -3, 1, 1, -3) \\ u_4 = \frac{1}{4}(1, 1, 1, -3, 1, 1, 1, -3) \\ u_5 = \frac{1}{4}(1, 1, -3, 1, 1, 1, 1, -3) \\ u_6 = \frac{1}{4}(1, -3, 1, 1, 1, 1, 1, -3) \\ u_7 = \frac{1}{4}(-3, 1, 1, 1, 1, 1, 1, -3) . \end{cases}$$

Then the Gram matrix $I=(\langle u_i, u_j\rangle)$ has non-zero determinant, i.e.

$$\det I=\frac{9}{2}=(\det E_7^*)\cdot 3^2 .$$

Hence $u_1, \cdots, u_7$ are linearly independent and generate a sublattice of index 3 in E_7^*. Letting

$$v=\frac{1}{3}\sum_{i=1}^{7} u_i=\frac{1}{4}(1, 1, 1, 1, 1, 1, 1, -7)\in E_7^* ,$$

we set

$$u_{ij}=u_i+u_j-v \qquad (1\leq i<j\leq 7) , \tag{5.5}$$

Then u_i and u_{ij} give all the 28 permutations of u_1. To simplify the notation, we denote them by

$$u_n\ (1\leq n\leq 28) \tag{5.6}$$

so that the 56 minimal vectors are given by $\{\pm u_n\}$. If we let $u_1'=u_{67}$, then E_7^* is generated by $u_1', u_2, \cdots, u_7$, since

$$v=u_6+u_7-u_1', u_1=3v-u_2-\cdots-u_7 .$$

All the roots of E_7 can be expessed as linear combinations of u_i. Explicitly,

$$\begin{cases} \alpha_1=u_2-u_1 , \\ \alpha_2=-u_4-u_5+u_6+u_7-2u_1' , \\ \alpha_i=u_i-u_{i-1} \quad (i=3, \cdots, 7) , \end{cases} \tag{5.7}$$

and hence all α_m $(m\leq 63)$ have similar expressions by (5.2).

Now the symmetric algebra over $E_7\otimes \boldsymbol{Q}$ can be identified with the polynomial ring $\boldsymbol{Q}[u_1, \cdots, u_7]$. From now on, we consider $u_1, \cdots, u_7$ as variables and regard u_n $(n\leq 28)$ and α_m $(m\leq 63)$ as the linear forms in $u_1, \cdots, u_7$ defined as above. Let

$$\varepsilon_\nu'=\nu\text{-th elementary symmetric function of } u_1^2, \cdots, u_{28}^2 . \tag{5.8}$$

By [S3], Theorem 7.2, we have

$$\boldsymbol{Q}[u_1, \cdots, u_7]^{W(E_7)}=\boldsymbol{Q}[\varepsilon_1', \varepsilon_3', \varepsilon_4', \varepsilon_5', \varepsilon_6', \varepsilon_7', \varepsilon_9'] . \tag{5.9}$$

The polynomial

$$\Delta_0(u)=\prod_{m=1}^{63} \alpha_m\in \boldsymbol{Q}[u_1, \cdots, u_7]$$

is a basic anti-invariant of $W(E_7)$, and its square

$$\delta_0=(\Delta_0)^2\in \boldsymbol{Q}[u_1, \cdots, u_7]^{W(E_7)} \tag{5.10}$$

is an invariant of weight 126 (playing the same role as the usual discriminant to the

symmetric group) which is in the statement (5) of Theorem 5. Observe that

$$\delta_0 \neq 0 \Longleftrightarrow \alpha_n \neq 0 \ (\forall n) .$$

Thus we sometimes say in this situation that there are *no vanishing roots.*

6. Construction of plane quartics with rational bitangents

Now we are ready for a systematic construction of plane quartics for which all the bitangents are defined over the field of definition of a given quartic.

THEOREM 11. *Letting $u_1, \cdots, u_7$ be independent variables over $\boldsymbol{Q}$, we set*

$$(6.1)\quad \begin{cases} q_4 = \dfrac{1}{36}\varepsilon'_1 \\ q_3 = \dfrac{1}{72}(-\varepsilon'_3 + 6084 q_4^3) \\ p_1 = \dfrac{1}{60}(\varepsilon'_4 - 43875 q_4^4 + 1800 q_4 q_3) \\ q_2 = \dfrac{1}{504}(\varepsilon'_5 - 238680 q_4^5 + 21600 q_4^2 q_3 - 1008 q_4 p_1) \\ p_0 = \dfrac{1}{540}(-\varepsilon'_6 + 1022580 q_4^6 - 165600 q_4^3 q_3 + 7008 q_4^2 p_1 + 10344 q_4 q_2 + 540 q_3^2) \\ q_1 = -\dfrac{1}{3828}(\varepsilon'_7 - 3552120 q_4^7 + 910800 q_4^4 q_3 - 11592 q_4 q_3^2 - 20592 q_4^3 p_1 \\ \qquad - 100824 q_4^2 q_2 + 7944 q_4 p_0 - 1092 q_3 p_1) \\ q_0 = \dfrac{1}{29496}(\varepsilon'_9 - 24667500 q_4^9 + 12751200 q_4^6 q_3 - 771120 q_4^3 q_3^2 + 683760 q_4^5 p_1 \\ \qquad - 2702280 q_4^4 q_2 + 145200 q_4^3 p_0 + 489288 q_4^2 q_1 - 224040 q_4^2 q_3 p_1 \\ \qquad + 61824 q_4 q_3 q_2 + 8760 q_3 p_0 + 1848 q_3^3 - 12656 q_4 p_1^2 + 5024 p_1 q_2) . \end{cases}$$

Let

$$\lambda = (p_0, p_1, q_0, q_1, q_2, q_3, q_4) ,$$

and consider the plane quartic Γ_λ defined by the equation (1.1). *Then its* 28 *bitangents are given by the lines*

$$(6.2)\qquad l_n : x_2 = (u_n^2 - q_4)x_1 + b_n x_0 \qquad (n = 1, \cdots, 28) ,$$

where, for each n, u_n is determined by $u_1, \cdots, u_7$ by the rule (5.6) *and b_n is a certain rational function of $a_n = u_n^2 - q_4$ with coefficients in $\boldsymbol{Q}(\lambda)$ which is also a polynomial in*

$\boldsymbol{Q}[u_1, \cdots, u_7]$. *In particular, all the* 28 *bitangents are rational over* $\boldsymbol{Q}(u_1, \cdots, u_7)$.

Proof. This is a "split" form of Theorem 7, 8 in §3 which is just a translation of the results on Mordell-Weil lattices of type E_7 (Theorem (E_7), Theorem 9.5 of [S3]) into the language of plane quartics by the dictionary explained in the previous sections.

N.B. Classically it is known as Aronholdt's theorem that given 7 general lines in a plane, there is a unique plane quartic such that these 7 lines form a maximal "azygetic" set of bitangents and such that the other 21 bitangents are constructed rationally from them (see [W], [vW]). The above theorem can be regarded as an explicit version of this classical result. It should be emphasized that the simplification is due to a very well-chosen coordinate system suggested by the viewpoint of Mordell-Weil lattices.

Next we drop the assumption that $u_1, \cdots, u_7$ are independent variables in the above result. In other words, we consider a specialization of u_i to arbitrary numbers, say to rational numbers c_i:

$$(u_1, \cdots, u_7) \longrightarrow (c_1, \cdots, c_7) \in \boldsymbol{Q}^7 .$$

Then Γ_λ becomes a plane quartic defined over $\boldsymbol{Q}$ and the above theorem gives an algorithm for the construction of plane quartics with rational bitangents. More precisely, we have:

THEOREM 12. *For any* $(u_1, \cdots, u_7) \in \boldsymbol{Q}^7$ *satisfying* $\delta_0 \neq 0$, *define* $\lambda = (p_i, q_j) \in \boldsymbol{Q}^7$ *by the formula* (6.1). *Then* Γ_λ *is a smooth plane quartic defined over* $\boldsymbol{Q}$ *all of whose* 28 *bitangents are rational over* $\boldsymbol{Q}$. *They are given by*

$$l_n : x_2 = a_n x_1 + b_n x_0 \qquad (n = 1, \cdots, 28) , \tag{6.3}$$

with $a_n = u_n^2 - q_4 \in \boldsymbol{Q}$ *and suitable* $b_n \in \boldsymbol{Q}$.

This is a translation of Theorem (E_7) of [S3] in the present setting (cf. Theorem 5 for the smoothness condition).

As an illustration, let us work out an explicit numerical example. By the above, we can choose $(u_1, \cdots, u_7) \in \boldsymbol{Q}^7$ almost arbitrarily; the only requirement is that $\delta_0 \neq 0$. But for an aesthetic reason, let us arrange the data so that the resulting quartic and the bitangents have equations with (relatively small) integral coefficients or with at most small denominators.

Example. Take

$$(u_1, u_2, \cdots, u_7) = (8, 9, 10, 11, 12, 13, 15) . \tag{6.4}$$

Then the 28 values $\{u_m\}$ of (5.6) rearranged in the increasing order are as follows:

(6.5)

$$\{-9, -8, -7^2, -6^2, -5^3, -4^2, -3^3, -2^2, -1^2, 0, 1, 2, 8, 9, 10, 11, 12, 13, 15\} ;$$

here -7^2 means for instance that -7 appears with multiplicity 2 among $\{u_m\}$. On the other hand, (5.7) gives the value of "simple roots":

$$(\alpha_1, \alpha_2, \cdots, \alpha_7)=(1, 1, 1, 1, 1, 1, 2)\,.$$

(Actually we chose α_i first and solved (5.7) to determine u_i.) Then all other α_m $(m\leq 63)$ are also positive integers, since they are linear combination of α_i $(i\leq 7)$ with nonnegative integer coefficients as in (5.2). In particular, there are no vanishing roots:

$$\delta_0\neq 0\,.$$

(N.B. This is a simple but useful device to attain nondegeneracy condition of Mordell-Weil lattices in a more general situation; cf. [S3], §3)

By the formula (6.1) of fundamental invariants, we have then

$$\begin{cases} q_4=38 \\ q_3=243542/3 \\ p_1=-1228331 \\ q_2=70216666 \\ p_0=-1646938126/3 \\ q_1=91398753794/3 \\ q_0=153529297476248/27 \end{cases}$$

This determines a plane quartic $\Gamma=\Gamma_\lambda$ defined over $\boldsymbol{Q}$ by the normal form (1.1). In order to get rid of denominators, let us choose the homogeneous coordinates $(X: Y: Z)$ of $\boldsymbol{P}^2$ such that

$$(x: t: 1)=(x_2: x_1: x_0)=(X: Y: 3Z)\,.$$

Then the defining equation of Γ is given by

$$\begin{aligned} &3X^3Z+X(Y^3-11054979YZ^2-14822443134Z^3)+38Y^4+243542Y^3Z \\ &+631949994Y^2Z^2+822588784146YZ^3+460587892428744Z^4=0 \end{aligned} \tag{6.6}$$

Let us determine the bitangents. For each value c in (6.5), there is a rational point $P=(at+b, ct^2+dt+e)\in E(\boldsymbol{Q}(t))$, which corresponds to a bitangent $X=aY+3bZ$. The value of a is uniquely determined by c as $a=c^2-q_4$. As for b, its expression as a rational function of a with coefficeints in $\boldsymbol{Q}(\lambda)$ does not always work because the denominator may vanish. It is more practical to go back to the relations (3.8) and (3.9), and determine d first as a common root of (3.9) for the value of c under consideration. The choice of d may not be unique, but once it is fixed, b is uniquely determined.

Indeed, if c appears among $\{u_m\}$ with multiplicity 1 and in addition, if $-c$ does not belong to $\{u_m\}$, then b is uniquely determined by a. In the present example, $c=10, 11, 12, 13, 15$ has this property. For instance, for $c=15$, we have $a=187$ and $d=246570$ (this d is the only rational solution of (3.9) in this case), which implies

$b=2330149/3$ and $e=684224475$. This gives the bitangent $X=187Y+2330149Z$.

On the other hand, if both c and $-c$ appear in (6.5) with multiplicity 1, then there are 2 bitangents having the same a. This is the case for $c=8$, $a=26$, or $c=9$, $a=43$. More generally, if $|c|$ appears with multiplicity μ among $\{|u_m|\}$, then there are exactly μ bitangents with the same $a=c^2-q_4$.

In this way, we can show that the plane quartic (6.6) has the following 28 bitangents, all rational over $\boldsymbol{Q}$, which are arranged in the increasing order of a.

(6.7)

$X+38Y+78926Z=0$	$X+13Y-37549Z=0$
$X+37Y+82331Z=0$	$X+2Y-13954Z=0$
$X+37Y+80315Z=0$	$X+2Y-41170Z=0$
$X+37Y+60155Z=0$	$X-11Y-26389Z=0$
$X+34Y+78686Z=0$	$X-11Y-46549Z=0$
$X+34Y+69326Z=0$	$X-26Y-35794Z=0$
$X+34Y+23246Z=0$	$X-26Y-55954Z=0$
$X+29Y+57731Z=0$	$X-43Y-72949Z=0$
$X+29Y+44771Z=0$	$X-43Y-80725Z=0$
$X+29Y-32989Z=0$	$X-62Y-125074Z=0$
$X+22Y+31166Z=0$	$X-83Y-228205Z=0$
$X+22Y+8990Z=0$	$X-106Y-428674Z=0$
$X+13Y+12851Z=0$	$X-131Y-787069Z=0$
$X+13Y-1549Z=0$	$X-187Y-2330149Z=0$

7. Remarks

(I). Classically the existence of plane quartics over $\boldsymbol{R}$ with 28 real bitangents is known (cf. [W]). But I have never seen any explicit example of a plane quartic over $\boldsymbol{Q}$ with rational bitangents in the literature. This is one of the motivations for the present paper. As is shown above, the construction of such an example can be done by a direct application of the method of Mordell-Weil lattices. It should be remarked that our construction is, in principle, the same as writing down an algebraic equation with a set of prescribed roots (cf. [S3], §1).

However, at the last moment of finishing this paper, I found a predecessor. In the paper [Br], Bramble solved the question, though he did not write down an example. Among other things, he carried out the construction by considering the net of plane cubics passing through 7 base points, the connection being (cf. the end of §2) that a del Pezzo surface of degree 2 is obtained by blowing up 7 points in general position in a projective plane. It is remarkable that interesting ideas from classical geometry are combined there with extraordinary strength of computation to produce beautiful results, at a time when a modern computer was not available.

We leave it to the reader to compare the method of Bramble with ours, but the following remark may be of some help. A linear pencil of plane cubics defines an elliptic surface over $\boldsymbol{P}^1$ where the base points give distinguished sections. When the

generic fibre is transformed to the Weierstrass form, the corresponding pencil is not linear any more, and these sections get the expression like (2.5). See [S6] where similar facts for E_8 (instead of E_7) are treated.

(II). The following subjects are naturally related to the contents of this paper, and they are to be discussed in some other occasion:

(i) Singularities of plane quartics and degeneration of Mordell-Weil lattices. The main idea for this is a systematic use of *vanishing roots* (cf. [S7]).

(ii) Plane quartics with a special flex and Mordell-Weil lattices of type E_6.

Starting from Proposition 2, we can develop a variant for type E_6 of what we have done above for type E_7. In this case, the flex tangent is a bitangent and the remaining 27 bitangents are represented by half of the 54 minimal vectors of the dual lattice E_6^*, which are also realted to 27 lines on a cubic surface (cf. [S5], §8, 2)).

References

[A] CONWAY, J. *et al.*; Atlas of Finite Groups, Clarendon Press, Oxford, (1985).

[Br] BRAMBLE, C.; A collineation group isomorphic with the group of the double tangents of the plane quartic, *Amer. J. Math.*, **XL**, (1918), 351–365.

[B] BOURBAKI, N.; Groupes et Algèbres de Lie, Chap. 4, 5 et 6, Hermann, Paris, (1968).

[CS] CONWAY, J., SLOANE, N.; Sphere Packings, Lattices and Groups, Springer-Verlag, (1988).

[K] KLEIN, F.; Über die Transformation siebenter Ordnung der elliptischen Funktionen, *Math. Ann.*, **14** (1978/79); Werke, vol. III, 90–136, Reprint: Springer-Verlag, (1973).

[L] LANG, S.; Fundamentals of Diophantine Geometry, Springer-Verlag, (1983).

[Ma] MANIN, Ju.; Cubic Forms, North-Holland, (1974).

[Mu] MUMFORD, D.; Curves and their Jacobians, Univ. Michgan Press, (1975).

[Se] SERRE, J.-P.; Lectures on the Mordell-Weil theorem, Vieweg, (1989).

[S1] SHIODA, T.; Mordell-Weil lattices and Galois representation, I, II, III, *Proc. Japan Acad.*, **65A**, (1989), 267–271, 296–299, 300–303.

[S2] SHIODA, T.; On the Mordell-Weil lattices, *Comment. Math. Univ. St. Pauli*, **39**, (1990), 211–240.

[S3] SHIODA, T.; Construction of elliptic curves with high rank via the invariants of the Weyl groups, *J. Math. Soc. Japan*, **43**, (1991), 673–719.

[S4] SHIODA, T.; Mordell-Weil lattices of type E_8 and deformation of singularities, in: SLN 1468, (1991), 177–202.

[S5] SHIODA, T.; Theory of Mordell-Weil lattices, Proc. ICM Kyoto-1990, vol. I, (1991), 473–489.

[S6] SHIODA, T.; An infinite family of elliptic curves over $\boldsymbol{Q}$ with large rank via Néron's method, *Invent. Math.*, **106**, (1991), 109–119.

[S7] SHIODA, T.; Existence of a rational elliptic surface with a given Mordell-Weil lattice, *Proc. Japan Acad.*, **68A**, (1992), 251–255.

[vW] VAN DER WAERDEN, B. L.; A History of Algebra, Springer-Verlag, (1985).

[W] WEBER, H.; Lehrbuch der Algebra, Vol. 2, Braunschweig, (1899).

Department of Mathematics,
Rikkyo University
Nishi-Ikebukuro,
Tokyo 171, Japan